Amendments to the Claims

1. (currently amended) A method of[[for]] transmitting secured data ~~over a wireless link~~, the method comprising:

utilizing a first key to encrypt ~~encrypting~~ a payload ~~according to a first session key~~;

adding a header to the encrypted payload to form a data packet;

utilizing a second key to encrypt ~~encrypting~~ the first ~~session~~ key;

utilizing a third key to encrypt ~~encrypting~~ the data packet ~~according to a second session key~~;

transmitting the encrypted first ~~session~~ key to a wireline device, wherein the wireline device decrypts the encrypted first key;[[and]]

transmitting the encrypted data packet over a wireless link to a gateway, wherein the gateway[[which]] decrypts the encrypted data packet to recreate[[,]] ~~recreates~~ the encrypted payload and the header, and forwards the encrypted payload and the header to the wireline device over an open network; and

utilizing the wireline device and the first key to decrypt the encrypted payload.

2. (currently amended) The method of claim 1, wherein the first ~~session~~ key comprises[[uses]] a symmetric key.

3. (currently amended) The method of claim 1, further comprising:

~~receiving the encrypted first session key and the encrypted payload at the wireline device;~~

~~decrypting the encrypted first session key; and~~

~~decrypting the encrypted payload using the decrypted first session key.~~

transmitting the encrypted first key to the wireline device, wherein the wireline device decrypts the encrypted first key using a private key associated with the second key.

4. (currently amended) The method of claim 1, wherein the third ~~second session~~ key comprises[[uses]] a symmetric session key.

5. (canceled).

6. (currently amended) A device for transmitting secured data over a wireless link ~~to a gateway providing access to a wide area network;~~, the device comprising:

an encryption engine which generates a first ~~session~~ key, encrypts a payload according to the[[a]] first ~~session~~ key, adds a header to the encrypted payload to form a data packet, encrypts the first ~~session~~ key according to a second key,[[;]] and encrypts the data packet according to a third ~~second session~~ key; and

a wireless transceiver coupled to the encryption engine, the wireless transceiver transmitting ~~which transmits~~ the encrypted first ~~session~~ key to a

server and transmitting ~~transmits~~ the encrypted data packet over the[[a]] wireless link to a gateway, wherein the gateway[[which]] decrypts the encrypted data packet to recreate~~, recreates~~ the encrypted payload and the header, and forwards the encrypted payload and the header to the[[a]] server over an open network;

wherein the server decrypts the encrypted first key and decrypts the encrypted payload using the decrypted first key.

7. (canceled).

8. (currently amended) The device of claim 6, wherein the payload comprises location information regarding a location of the ~~wireless~~ device.

9. (currently amended) The device of claim 6, wherein the first key ~~encryption algorithm~~ employs a symmetric key.

10. (currently amended) A method for secured communication between a mobile device and a server on a wide area network, the method comprising:

encrypting a payload at the mobile device using a first session key;

encrypting the ~~an unencrypted~~ first session key at the mobile device using a public key;

transmitting the encrypted first session key to the server over a wireless

link;

decrypting the encrypted first session key at the server;

~~encrypting a payload at the mobile device using the unencrypted first session key;~~

adding a header to the encrypted payload to form a data packet at the mobile device;

encrypting the data packet according to a second session key configured for secured communications over the wireless link; and

transmitting the encrypted data packet from the mobile device to a gateway which decrypts the encrypted data packet to recreate~~, recreates~~ the encrypted payload and the header, and forwards the ~~decrypted~~ encrypted payload and the header to the server;

wherein the server utilizes the decrypted first session key to decrypt the encrypted payload.

11. (currently amended) The method of claim 10~~, further comprising:~~

~~receiving the encrypted data packet at the gateway;~~

~~decrypting the encrypted data packet at the gateway to recover a decrypted data packet comprising the encrypted payload encrypted with the first session key;~~

~~forwarding the decrypted data packet to the server over the wide area network;~~

~~decrypting the encrypted first session key at the server using a private~~

~~key; and~~

~~decrypting the encrypted payload at the server using the decrypted first session key.~~

wherein the decrypting the encrypted first session key at the server further comprises:

decrypting the encrypted first session key at the server using a private key associated with the public key.

12-14. (canceled).

15. (original) The method of claim 10, wherein the payload includes location information.

16. (currently amended) The method of claim 10, ~~wherein the~~ further comprising:

generating the[[a]] first session key at the mobile device ~~further comprises generating the first session key~~ based on a random number.

17. (currently amended) The method of claim 10, wherein the encrypting the[[a]] payload at the mobile device using the first session key further comprises:

encrypting the payload at the mobile device using the first session key, wherein the first session key employs an encryption algorithm selected from a

group of ~~at least one of the~~ encryption algorithms consisting of DESX and[[or]] DES.

18-19. (canceled).

20. (currently amended) The method of claim 1, ~~wherein~~ further comprising:

implementing an encryption algorithm selected from a group of encryption algorithms consisting of ~~the first session key implements at least one of the encryption algorithms~~ DESX and[[or]] DES.

21-24. (canceled).

25. (previously presented) The method of claim 1, wherein the data packet includes location information.

26. (currently amended) The method of claim 1, further comprising:

utilizing a random number to generate the first key.

~~4, wherein the first session key is generated based on a random number.~~

27. (currently amended) The device of claim 6, further comprising:

a memory coupled to the encryption engine, wherein the memory ~~having a public key associated with a server on the wide area network stored therein~~

stores the second key, and wherein the encryption engine accesses the second key from the memory.

28. (canceled).

29. (currently amended) A computer readable medium[[,]] comprising program instructions for performing a method comprising:

encrypting a payload according to a first ~~session~~ key;

adding a header to the encrypted payload to form a data packet;

encrypting the first ~~session~~ key according to a second key;

encrypting the data packet according to a third ~~second session~~ key configured for secured communications over a wireless link;

transmitting the encrypted first ~~session~~ key to a server; and

transmitting the encrypted data packet over the[[a]] wireless link to a gateway, wherein the gateway[[which]] decrypts the encrypted data packet to recreate~~, recreates~~ the encrypted payload and the header, and forwards the encrypted payload and the header ~~over an open network~~ to the server, and wherein the server[[which]] decrypts the encrypted first ~~session~~ key and decrypts the encrypted payload using the decrypted first ~~session~~ key.

30. (currently amended) The computer readable medium of claim 29, wherein the first ~~session~~ key comprises[[uses]] a symmetric key.

31. (currently amended) The computer readable medium of claim 29, wherein the method further ~~comprising~~ comprises:

receiving the data packet at the gateway;

decrypting the data packet at the gateway according to the third ~~second session~~ key;

forwarding the encrypted payload to the server;

receiving the encrypted first ~~session~~ key at the server;

decrypting the encrypted first ~~session~~ key using a fourth ~~private~~ key; and

decrypting the payload according to the decrypted first ~~session~~ key.

32. (currently amended) The computer readable medium of claim 29, wherein the first ~~session~~ key comprises[[uses]] a symmetric session key.

33. (currently amended) The computer readable medium of claim 29, wherein the method further ~~first session key~~ comprises:

implementing an encryption algorithm selected from a group of ~~at least one of the~~ encryption algorithms consisting of DESX and[[or]] DES.

34. (previously presented) The computer readable medium of claim 29, wherein the data packet includes location information.

35. (previously presented) The computer readable medium of claim 32, wherein the symmetric session key is generated based on a random number.